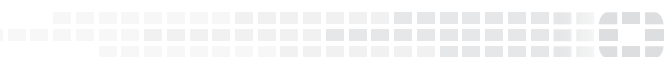




*High Performance Network Security*



# FortiAnalyzer Upgrade Guide

**VERSION 5.2.8**

**Copyright© 2016 Fortinet, Inc. All rights reserved.**

Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

# 1

## Overview

## **STEP 1: Before You Begin**

Make sure FortiAnalyzer 5.2.8 can run on your FortiAnalyzer model. Back up your device configuration and logs. Wait until all the running reports are completed.

## **STEP 2: Download**

Download upgrade images from Fortinet [Customer Service & Support portal](#).

## **STEP 3: Upgrade and Monitor**

Install the new firmware and monitor the rebuild process.

## **STEP 4: Verify**

Verify the upgrade has been completed successfully.

# 2

## Upgrade Paths

You can upgrade FortiAnalyzer 5.0.6 or later directly to FortiAnalyzer 5.2.8.

If you are upgrading from 5.0.5 or earlier, you will need to upgrade to FortiAnalyzer 5.0.6 first.

Initial Version	Upgrade To	Log Database Rebuild Required?
5.2.0 or later	5.2.8	No
5.0.6 or later	5.2.8	Yes for 5.0.6, No for the rest
5.0.5 or earlier	5.0.6	Yes

# 3

## Detailed Upgrade Instructions

## Step 1. Back Up Your Device.

- Make sure FortiAnalyzer 5.2.8 can run on your FortiAnalyzer model. For a list of FortiAnalyzer models that support FortiAnalyzer 5.2.8, see “Supported Models” on page 12.
- Back up your device configuration and logs.
- Wait until all the running reports are completed. Use the following CLI commands to check for running and pending reports.

```
FAZ1000D # dia report status running
```

```
FAZ1000D # dia report status pending
```

- If you are upgrading a FortiAnalyzer VM, make sure your VM partition has more than 512MB\*, and your VM server is up to date.

## Step 2. Download.

Download upgrade images from Fortinet [Customer Service & Support portal](#).

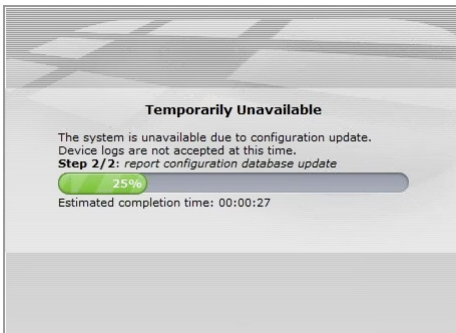
*\*It is recommended to allocate 1024MB for the FortiAnalyzer VM partition.*



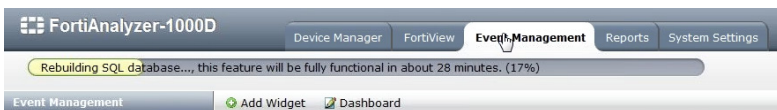
## Step 3. Upgrade and Monitor

Install the downloaded firmware image.

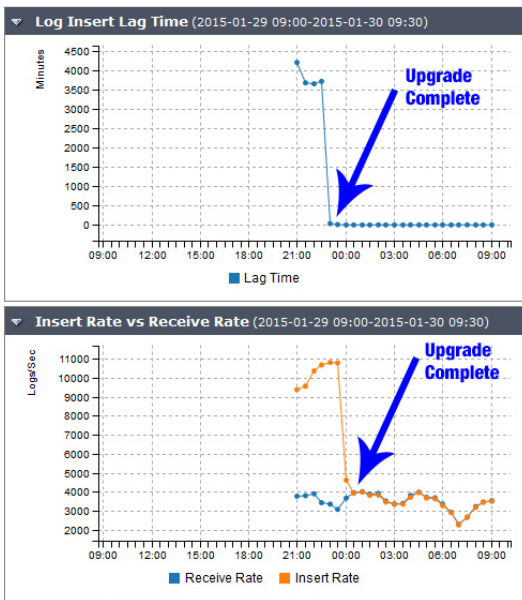
During a firmware upgrade, your FortiAnalyzer will be temporarily disconnected from your management computer. When the firmware has been installed, the FortiAnalyzer is connected again.



When complete, log in to your FortiAnalyzer. Not all features will be available while the SQL database is rebuilt. A status bar will keep you up to date on the rebuild status:



Monitor the rebuild progress with the Log Insert Lag Time and Insert Rate vs Receive Rate widgets. These widgets will show you the gap between logs being received and logs being inserted after the upgrade. You can customize this widget to show data every 60 to 240 seconds. As shown below, you will notice an initial delay in logs being inserted, but that will resolve itself as time passes. You can add these widgets in the same way you add other widgets in the Dashboard.



## Step 4. Verify

Verify the following to make sure the upgrade has been completed successfully.

1. Database rebuild is successful. Use this CLI command to check database rebuild:

```
diag sql status rebuild-db
```

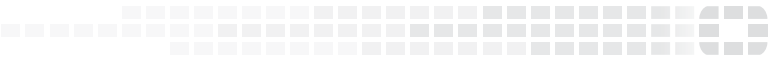
2. Configurations are not lost.
3. Launch Device Manager and make sure that all the log devices that were added previously are still listed.
4. Launch other functional modules and make sure they work properly.

# Supported Models

FortiAnalyzer	FortiAnalyzer VM
FAZ-100C	FAZ-VM64
FAZ-200D	FAZ-VM64-AWS
FAZ-300D	FAZ-VM64-HV
FAZ-400C	FAZ-VM64-KVM
FAZ-400E	FAZ-VM64-XEN
FAZ-1000C	(Citrix XenServer and Open Source Xen)
FAZ-1000D	
FAZ-1000E	
FAZ-2000B	
FAZ-2000E	
FAZ-3000D	
FAZ-3000E	
FAZ-3000F	
FAZ-3500E	
FAZ-3500F	
FAZ-3900E	
FAZ-4000B	

**FORTINET®**

*High Performance Network Security*



05-528-382729-20160826